Getronics
Business Continuity

Interfacing ITIL change management and contingency planning

Version:	1.0 (DRAFT)
Date:	November 1998
Author:	Ernst J. Oud
File:	\Data\Word\BCP Change Management 01.doc

Table of contents

1. INTRODUCTION 3

1.1. Disaster Recovery Methodology 3

2. KEEPING THE CONTINGENCY SYSTEM UP TO DATE 4

2.1. Preventive maintenance 4
2.2. Regular testing and corrective maintenance 5
2.3. Contingency audits in the operational phase 5

3. IMBEDDING PREVENTIVE MAINTENANCE 6

3.1. IT control systems 6
3.2. The link between change management and a contingency system 7
3.3. Configuration Management Data Base (CMDB) 12

4. CHANGES IN BUSINESS PROCESSES OTHER THAN IT 13

5. FURTHER READING 14

1. Introduction

Evaluating contingency plans of customers and the way these plans are imbedded within the organisation, it seems that the most daunting task facing contingency managers is trying to keep the plan updated. Apparently the business arena has become too dynamic to keep up with. In fact the pace of change is that high that trying to get a contingency plan updated has almost become impossible. Making sure that everyone involved, for instance the members of the emergency teams, know what to do when disaster strikes almost certainly takes longer than the time an IT infra-structure is left unchanged. Certainly something needs to be done.

1.1. Disaster Recovery Methodology

Before trying to picture a solution, let me propose a working model[1] of how to build an operational contingency *system* (the constellation of contingency plan, organisational structure and back-up provisions).

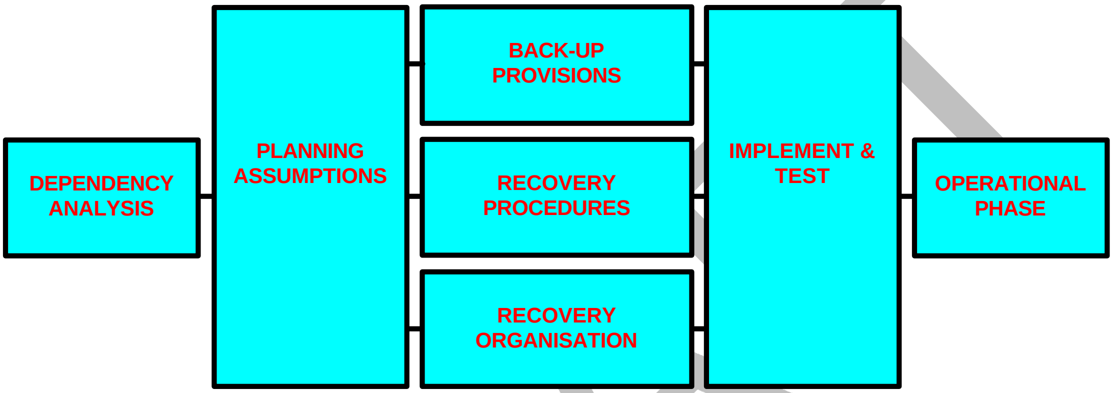


Figure 1 : Disaster Recovery Methodology™

Figure 1 depicts the Disaster Recovery Methodology (DRM) used by Getronics Business Continuity BV to build and maintain an operational contingency system. As shown, a DRM project consists of a number of phases. Phase one, the dependency analysis, evaluates the critical business processes and executes a risk-analyses or Business Impact Analysis for those processes.

Within phase two, the planning assumptions for the contingency plan are investigated; for instance the maximum allowable downtime and worst case scenario are researched and the priorities of the business processes and the required number of workplaces during an emergency are determined. These assumptions form the basis for the next phases in which the actual contingency system is built.

Back-up provisions have to be put in place for all the required means to keep the critical business processes running, like ICT, office space and logistics. Recovery procedures consist of the escalation procedures, which explain how a seemingly small problem has to escalate to the point where the processes evacuate to the back-up facility (who to inform, how are decisions taken, which time-frame to use) and the handbook that describes all the technical steps to be taken during the actual evacuation process (how to IPL systems, how to restore data, how to reconfigure the network).

A recovery organisation consists of all the teams involved during the actual evacuation and recovery process. It might look like this:

[1] DRM is used as an example here. There are a number of other models available, for instance the ‘Business Continuity Planning Model’ - see http://www.dr.org/model.htm

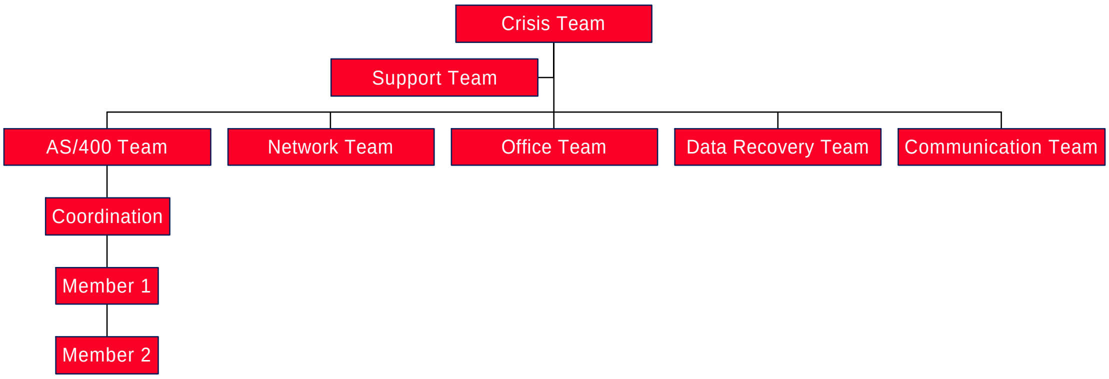


Figure 2 : Part of a sample recovery organisation

With operational back-up provisions, working procedures and a recovery organisation, a full implementation test will investigate whether the planning assumptions are being met; for instance whether everything put in place will restore the critical business processes within the maximum allowable downtime.

A detailed description of all the phases of DRM can be found within the DRM Project Manual (available in English) but is beyond the scope of this article. Basically the last DRM phase, the operational phase is most important for us now; within this phase the company or organisation has a fully implemented contingency system that should be kept up to date.

2. Keeping the contingency system up to date

The following paragraphs describe the three possible ways to keep the contingency system up to date:

- Preventive maintenance
- Corrective maintenance
- Contingency audits

The next chapter explains how to imbed the preventive maintenance of the contingency system within the IT control processes.

2.1. Preventive maintenance

A back-up facility which is not regularly maintained will lose, in time, its guaranteed availability in the event of a disaster; after all the production environment usually changes rather rapidly. Without maintenance, the scenario (consisting of a visual presentation of all steps to be taken and the list of actions) will be out of date in a relatively short time. Because tests are not run every day, there is no “automatic” alert to errors.

If the implications of a test evaluation are not incorporated into the back-up scenario immediately after a test, the vulnerability is increased unnecessarily. If a test fails (in whole or in part), this will happen during a real back-up operation too, unless the solutions to the problems which were encountered are incorporated into the scenario in time.

Software aids not only play an important role in the design and build-up of the back-up scenario, they also are a very handy tool for the maintenance of the scenario. Who or which department will be responsible for the maintenance of both the scenario and the manual is stipulated in the planning assumptions.

It is preferable that the responsibility for keeping these essential documents up to date is given to the same people or department who are responsible for their maintenance.

Changes in the manual and/or the scenario can be made necessary by:

- **The test results:** these are laid down in a test evaluation following every test.

- **New requirements**: new ideas with regard to critical applications should be brought in via the usual procedure within the organisation.

- **Changes in the daily production:** should be reported via the usual procedure within the organisation.

- **New hardware or system software**: should be reported via the usual procedure within the organisation.

- **Changes in the planning assumptions**: this means that part of the Disaster Recovery Methodology phases must be repeated. Take care that no new systems are made operational without investigating the consequences for a back-up operation.

2.2. Regular testing and corrective maintenance

After all the DRM phases have been run through, the organisation is prepared, in principle, to cope with a disaster. However, in order to prepare everyone for his or her task as thoroughly as possible, it is necessary to carry out a test one or more times a year. Such a test always reveals aspects that were given insufficient consideration during the preparatory phase. In this way, the back-up scenario can be optimised further. Regular testing of the back-up facility provides the highest degree of reliability for the success of a real back-up operation.

The following could be subjects of tests:

- The physical back-up facilities, especially the configuration and network facilities as described in the back-up manual.
- Activating the operating system and the subsystems.
- The back-up scenario.
- Restoring the application environment.
- Logistics (to the extent possible).
- Users' groups.

The first three must always be included in the test. Applications and selected users' groups can be tested in rotation. Users' groups are involved in the testing of a real 'end-to-end' situation. The usual procedure is that they are asked to shut down their normal activities a half-hour earlier than usual and then work on the back-up system for one hour. The planning of the back-up test in the back-up centre and the necessary network actions must be adjusted accordingly.

Logistic procedures are generally only involved in incidental 'real-life' tests. These are regular tests in which both your own organisation and external suppliers (logistics) are unexpectedly confronted with a disaster.

The planning, preparation and execution of the regular test procedure constitute part of the 'maintenance' of the back-up facility.

2.3. Contingency audits in the operational phase

The auditing procedure can be set up by analogy with the ISO/9000 method. The principle of the auditing procedure is that 'internal' audits are held by one's own organisation and 'external' audits by an external body.

The organisation chooses an external body that has sufficient authority in the field of disaster planning to qualify as an auditing body.

The auditing procedure (the content and frequency of both the internal audits and the external audits) is discussed and established in consultation with the external body. The guideline must be that all parts of the back-up facility have to be subjected to an internal audit at least once a year.

The number and extent of the external audits can be kept to a minimum by formalising the notation of the results and the follow-up of the internal audits. The internal audits then provide the basic material for the external audits, although the external body must of course have the authority to test arbitrary aspects of the disaster plan at random.

When drawing up the content of the internal audit, attention must be given to the aspects listed below. As a first approach, these aspects can be measured and evaluated 'in-house', although special demands will then be made of the back-up test and additional information will be requested from the users. The users concerned must also be involved in the audit, which must therefore not be limited to the IT department (danger of a 'professional blind spot').

- **Facilities and procedures for back-up and off-site storage**
- **Back-up provisions and procedures**
- **Users' aspects**
- **Maintenance of the back-up provisions and procedures**

Table 1 : Aspects to be included within an audit

3. Imbedding preventive maintenance

It can be debated that due to the dynamics of business processes corrective maintenance is not to be relied upon. Firstly when one needs corrective maintenance the organisation was clearly at risk; apparently the contingency system was sub-optimal. Secondly most organisations, wrongly or not is not the point here, do not prioritise contingency planning highly. In other words; corrective maintenance most of the time does not happen.

This does not suggest that corrective maintenance of a contingency system should not be done; especially when an organisation relies on third parties, like a commercial back-up provider, they would like to test whether those parties keep to their contract and if not correct the contingency system.

However for most purposes preventive maintenance of a contingency system seems the goal to strive for. By some way, the organisation should try to incorporate or imbed the control mechanisms to keep the contingency system updated within the overall IT control processes.

3.1. IT control systems

For IT control there are a number of systems like ITIL (IT Infrastructure Library - maintained by the British CCTA, see http://www.ccta.gov.uk) and CobiT (Control Objectives for IT - maintained by the American EDP organisation ISACA, see http://www.isaca.org).

Both ITIL and CobiT describe IT control objectives for controlling IT oriented business processes. Both recognise Contingency Planning as an important IT process.
The ITIL module Contingency Planning does not describe in detail how to imbed this control within other ITIL modules like Change Management, Problem Management and Service Level Management. ITIL however mentions that an important link exists with the process of change management.

Since the various ITIL modules itself do not clearly define how the ITIL processes interact, a number of organisations have devised methods of interfacing the various ITIL modules, one of these methods is Quint Wellington Redwood's **IPW** (**I**mplementation **P**rocess **W**orkflow) model. See figure 3 for the relevant part of the IPW model.

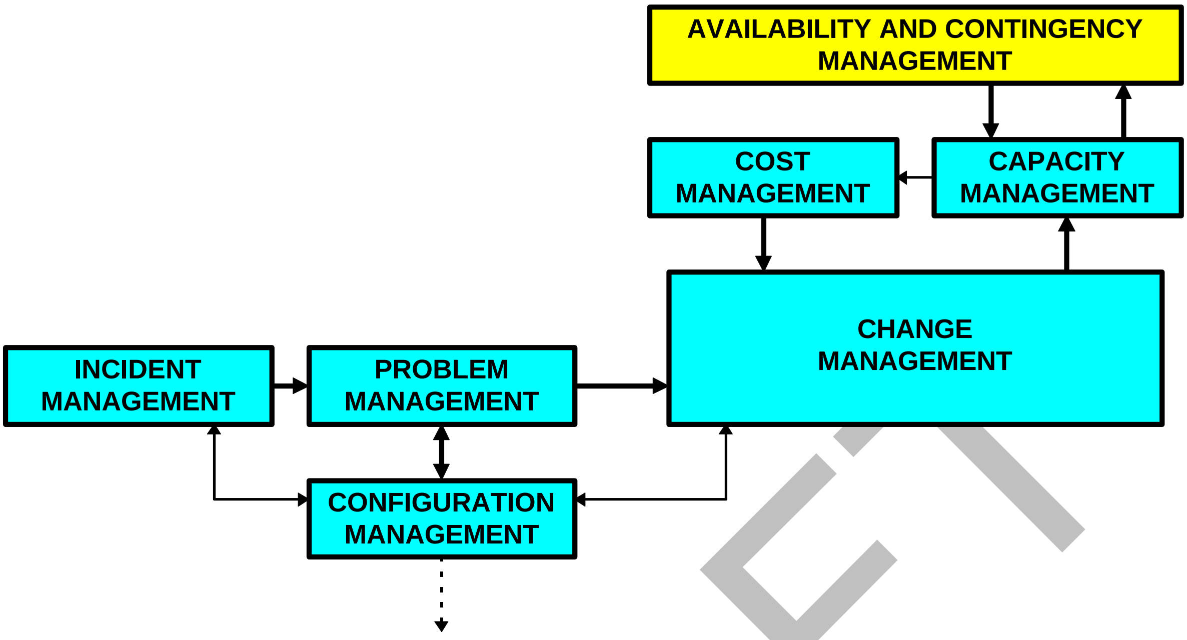


Figure 3 : Part of the IPW model

CobiT high-level control DS4 (Delivery and Support) deals with *"control over the IT process of ensuring continuous service"* and contains the control objective:

> **Maintaining the Information Technology Continuity Plan**
> CONTROL OBJECTIVE
> Information services function management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.

Apparently both ITIL and CobiT emphasise the importance of a link (imbedding) between a contingency system and change control procedures. Within the following ITIL is taken as a guideline but most of the material discussed applies to CobiT also.

3.2. The link between change management and a contingency system[2]

It should be pointed out that this paragraph deals with changes for which a formal change management system is in place. An organisation that adopts a formal change management system probably starts by implementing such a system for its ICT processes.
Therefor changes in the ICT infrastructure are assumed in this paragraph; not those changes within the business processes themselves or changes that deal with human resource management for instance. Nevertheless the next chapter will try to indicate how to deal with those changes when an impact on the contingency system is viable.

A formal system for change management will only allow changes that are authorised. It is therefor required that a proposed change is formally processed, see figure 4.

[2] Note that within the IPW model this link is formed via the ITIL process capacity management.

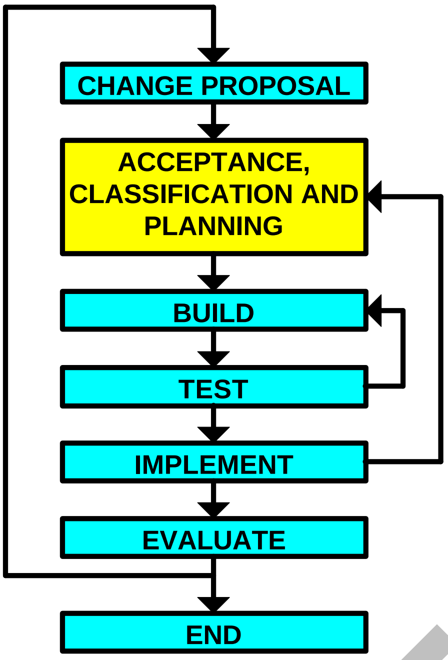


Figure 4 : Flow of a change according to ITIL Change Management

In reference to figure 4, our focus here lies with the 'acceptance, classification and planning' step[3]. Recently ISACA has published a *"Flowchart with CobiT References"* for the *"Internal Control Components in the Change Management Process"*. Where ITIL Change Management does not contain a direct link to Contingency Planning, this new *Flowchart* does; see figure 5.

[3] CobiT acknowledges *"identification, categorisation, prioritisation, impact assessment and authorisation of changes as well as release management and distribution"*.

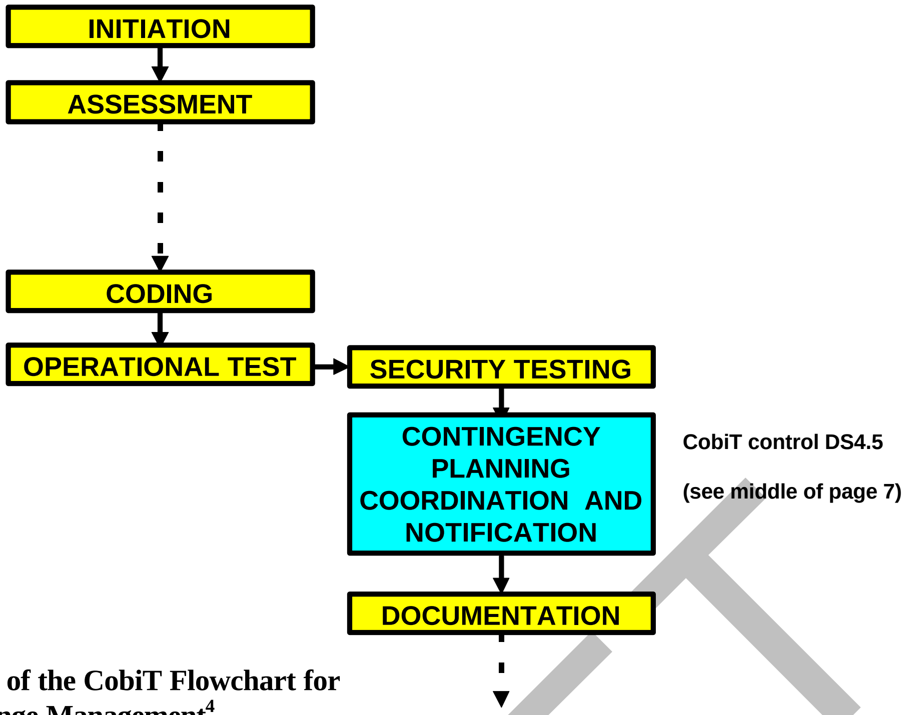


Figure 5 : Part of the CobiT Flowchart for Change Management[4]

A change proposal shall only be generated via a pre-defined procedure (for instance by entering a record in a dedicated database or in the configuration management database) by a limited number of employees; for instance the change manager, the configuration manager or the manager responsible for the helpdesk.

A change proposal should clearly describe to which system(s) the change applies. From the configuration management database it is then possible to determine which impacts the proposed change has on any other system.

When a change proposal has been received it has to be classified. Classification involves investigating the impact the change has on the organisation, budget, human resources ***and whether the continuity of the organisation is at risk by the proposed change.***

The number of levels for classification should be kept minimal, perhaps in the terms of ‘minor impact’, ‘reasonable impact’ and ‘major impact’. ***For each of these classifications the impact on the continuity of the organisation should be determined.***

After classification the change proposal should be authorised and incorporated within the planning for pending changes. Authorisation itself can be a three step process whereby management has to decide on changes that were classified as having ‘major impact’, the change manager authorises[5] changes classified as having ‘minor impact’ and a change committee decides on the changes that were classified as having ‘reasonable impact’.

To be able to decide whether to authorise the change, the change manager, management or the change committee should be able to determine whether the continuity of the organisation is impacted by the proposed change and whether a change to the contingency system is required. This implies that the person or department responsible for contingency planning need to be involved in this change authorisation process for two reasons; firstly to share their expertise on the impact of changes with the mentioned parties and secondly to be informed of changes that require a change in the contingency system.
The contingency manager therefor will need to be involved within the authorisation process itself; either within the change committee and/or within management of the organisation.

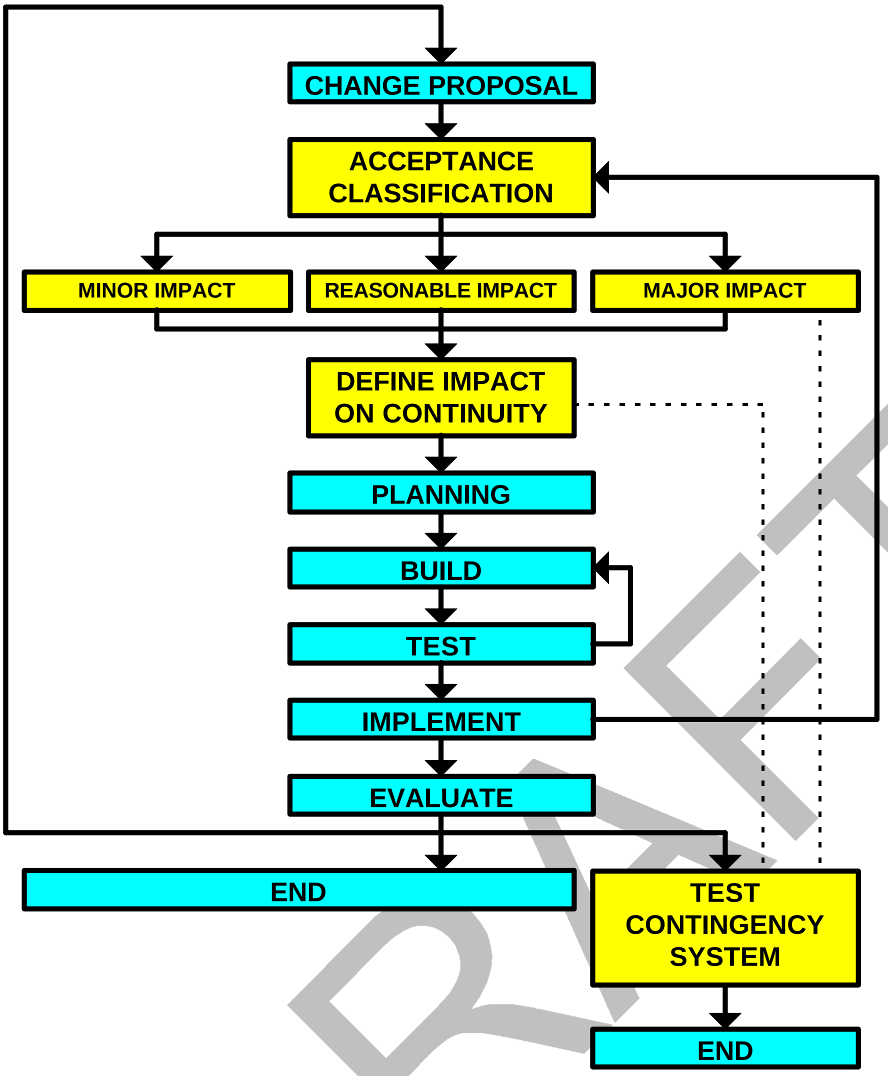
[4] For the full chart see http://www.isaca.org/flchrt1.htm

[5] Ofcourse he/she will consult others for advice.

Any changes that are classified as having a 'major impact' should lead to a detailed retest of the contingency system.

The contingency manager should have full access to the configuration management database so that authorised changes can be listed and the required changes to the contingency system be determined, planned and executed.

The flow of a change proposal thus becomes as follows:



When an impact is expected the contingency system needs to be updated …

… and when the change itself has a major impact the contingency system needs a full test.

Figure 6 : Adopted flow for change proposals

Notes:

- When an impact of a change on the contingency system is determined the required changes to the contingency system need to be processed as formal changes as well; i.e. the interface between contingency planning and change management works both ways.
- With changes where a major impact on the organisation is expected, a full test of the contingency system is an automatic consequence.
- With changes where minor or reasonable impact on the organisation is expected, the decision whether a test of the contingency system is required is left to the contingency manager.
- During the evaluation step it might become clear that the actual implementation of the change makes a test of the contingency system necessary. Perhaps earlier this was not seen as required but the chosen solution perhaps now changes this view.
- The contingency manager should be aware that a change in the IT infrastructure could have impact on his back-up provisions, procedures and recovery organisation.

Notes (continued):

- The contingency of an organisation is at risk most when implementing 'major impact' ***urgent*** changes. Practice has shown that because of the urgency not all precautions, like overseeing all possible side-effects, are taken. The contingency manager should be very much involved in the process that handles urgent changes.
- In reference to the previous note; implementing a change can fail. Especially when changes with 'reasonable impact' or 'major impact' are implemented, an emergency procedure for backing out should be developed. It should contain all necessary steps to reset all systems applicable to their previous state. It is obvious that implementing such a change and developing the back-out plan requires full involvement of the contingency manager and his team.
- The ITIL module Problem Management[6] deals with processing, registering and managing problems. To solve a problem a change to an IT system may be required. This implies that an indirect link between Contingency Planning and Problem Management exists.

3.3. Configuration Management Data Base (CMDB)

The previous paragraph mentions the configuration management data base as the container for all configuration data as well as change records to that configuration. The following describes possible add-ons to the database to ease monitoring of changes with impact on the contingency system.

Every Configuration Item (CI) record in the CMDB contains a status field, which indicates the current usage status of this CI, like 'operational', 'in test' or 'in service'. This field could also contain an instance like 'change pending' which would indicate to a contingency manager that a change proposal exists for this CI. Of course some sort of index to the change proposal itself needs to be included in this CI record also. At least owner and history of the proposal in question must be traceable. Preferably change proposals should also be stored in the CMDB.

An example (relational) CMDB would store the following information for every CI:

```
CI ID                              model/type
serial number                      location
category                           owner
status                             supplier
version                            comment
change proposal ID
```

Also within the CMDB for every CI the following relations would have to be specified:

```
is hierarchical submissive to      is part of
is connected to                    is a copy of
uses                               refers to
```

The field `status` would indicate whether a change proposal exists for this CI and via the relations the impact on other CI's can be found. The change proposal itself can be found using the field `change ID` as an index within the CMDB (provided it is built within a flexible relational database system).

Any contingency manager with access to such a CMDB has all the tools to know what changes are pending and which components are affected. Of course it is still up to the contingency manager to decide his plan of action for updating the various components of the contingency system (provisions, procedures, organisation) such that the contingency system will reflect the change.

[6] Most problems are reported by users to the helpdesk; which is described in the ITIL module Helpdesk.

4. Changes in business processes other than IT

Chapter 3 dealt with changes in the IT infrastructure for which a formal change management has been put in place. For those changes that occur in other business processes or for which no formal change process exists, other controls are required.

When no formal system for classifying changes exist the following changes have impact on phases of DRM and therefor on the contingency system:

Sort of change	DRM phase impacted
Any change with impact on critical business processes	Dependency analysis, Planning assumptions
Any change within the ICT infrastructure	Back-up provisions, Recovery procedures
Any change within personnel	Recovery organisation

Table 2 : Impact of changes on DRM phases

The person responsible for the contingency system (i.e. the contingency manager) should decide together with management whether the DRM phases mentioned in table 2 above should be restarted. If the change in some business process changes the criticality of other processes for instance, the dependency analysis need to be redone.

When no formal system for implementing changes exist, the contingency manager either needs to be very much involved within most of the processes within the organisation (i.e. he/she should be member of the management team) or the managers responsible for managing change should recognise the importance of reporting changes to the contingency manager. In both cases regular audits on the contingency system as well as tests are required. The function description of the managers responsible for implementing change should contain a description of their responsibility in keeping the contingency manager informed.

5. Further reading

DRM Project Manual (English / Dutch)
Getronics Business Continuity BV
http://www.getronics.nl/gbc

Operationeel beheer van Informatiesystemen (Dutch)
Kluwer Bedrijfsinformatie
Sander Koppens / Bas Meyberg
ISBN 90 267 1841 1

ITIL Module Contingency Planning (English)
Central Computer & Telecommunications Agency
http://www.ccta.org

Continue beschikbaarheid van de geautomatiseerde informatievoorziening (Dutch)
Nederlands Genootschap voor Informatica (NGI)
ISBN 90 267 1959 0

Code of Practice (British Standard 7799 - English)
British Standards Institution
http://www.bsi.org

Code voor Informatiebeveiliging (Dutch)
Nederlands Normalisatie Instituut
http://www.nni.nl

IPW (English)
Quint Wellington Redwood
http://www.quint.nl/index_uk.htm